

Note for readers of this English translation

This document has been translated from the Japanese original for reference purpose only. In the event of any discrepancy between this English translation and the Japanese original, the Japanese original shall prevail.

Business Briefing on IIJ Security Business




February 24, 2022
Internet Initiative Japan Inc.
Security Division
Mamoru Saito



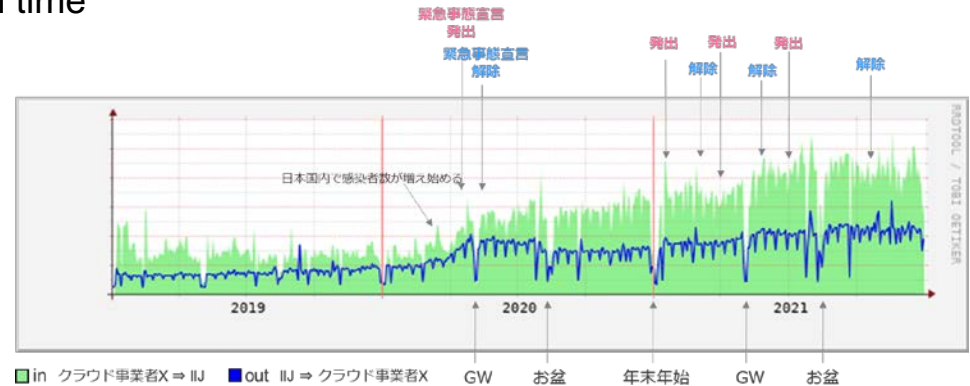
Trend of Threats in this one year

Impacts of the COVID-19 Pandemic
Incidents concerning outsourcing contractors
Safety of Cloud Services
Vulnerabilities of IoT Devices
DDoS attacks related to blackmail and/or social situation
Ransomware



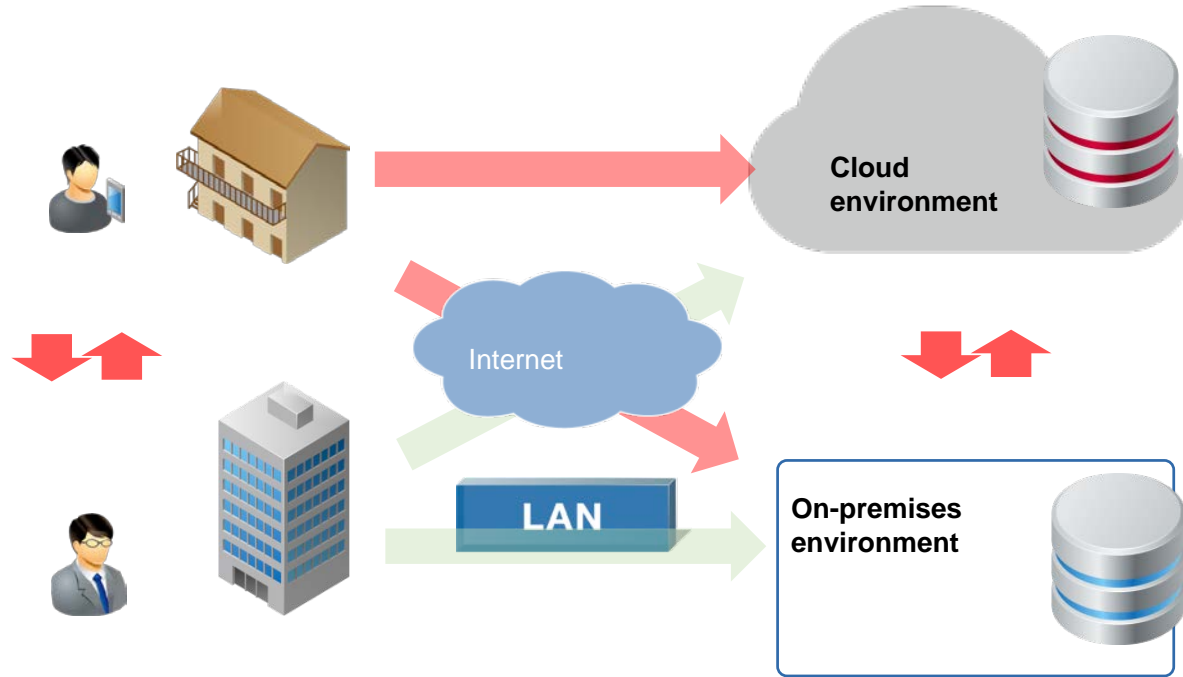
Impacts of the COVID-19 pandemic

- Various changes on the network
 - Increase of traffic related to teleworking (significant increase between February and June 2020)
 - Changes in traffic directions and changes in time
 - Video streaming services
 - Regional difference
- Changes in the ways to work
 - Teleworking
 - Increase in remote meetings
 - Remote international meetings
 - Decrease in client entertainment
 - Diversification of working locations (office, home, satellite office)
 - Relations with people whom one has met only virtually



Jan. 2022 “Business briefing on IIJ’s New Remote Access Service”
Change in traffic volume between a certain Cloud service provider and IIJ

Impacts of the COVID-19 pandemic

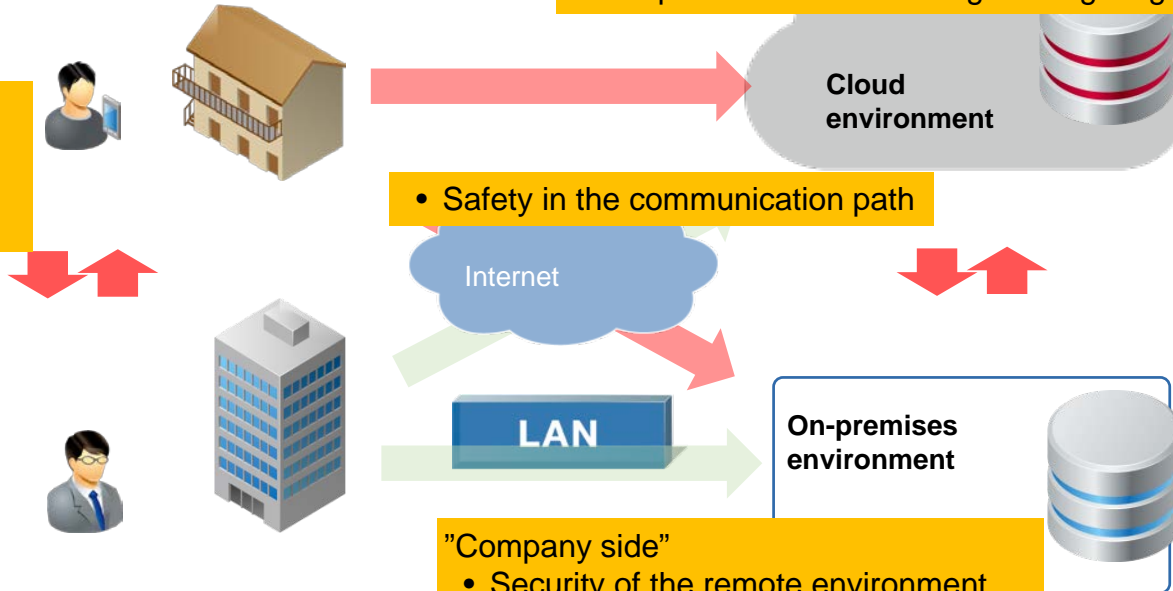


Impacts of the COVID-19 pandemic

- Reliability of cloud services
- Configuration of cloud services
- Acquisition and monitoring of usage logs of cloud services

"Employees"

- Working style at home
- Safety of the home IT environment



• Safety in the communication path

"Company side"

- Security of the remote environment
- Control of employees' works
- Events that cannot take place online

Incidents concerning outsourcing contractors

A type of so-called supply chain attacks. The incidents involve outsourcing contractors who build and operate software packages and systems for business uses

- A backdoor was deployed into a certain version of an U.S. IT operation management tool
Up to 18,000 organizations, including the federal agencies, were affected.
- Unauthorized accesses were made to a domestic electric company via a system operating company
 - The hacker made the accesses via the IT system operation monitoring service provided by the system operating company. The hacker took advantage of vulnerability in the software used for system operations and disclosed the information on the hacked servers.
- Information leak from an information sharing tool used by a major system integrator
 - Unauthorized accesses were confirmed in a part of the tool used for sharing information with internal/external parties.
 - Information related to over 100 domestic organizations was disclosed.
- U.S. system operation companies largely infected by ransomware
 - A vulnerability in a remote monitoring/management product was exploited and a little less than 60 system operation companies who were using this product were attacked. As many as 1,500 of their customer organizations were infected by the ransomware.

Safety of Cloud Services

- There are more jobs conducted by using a cloud service
- There are more jobs conducted on smartphones, tablets and other devices that process information through cloud computing
- Configuration errors and vulnerabilities in cloud services pose serious problems
 - Information leak caused by defective configuration related to guest users of a major cloud service
 - Information is likely to be leaked to a third party when excessive authority is given to guest users.
A cloud service provider claims that it is caused by a defective configuration by a user.
 - Due to a configuration error of a major cloud service provider, the personal information of 38 million customers was disclosed.
 - There are vulnerabilities in DBs provided by major cloud service providers. It is necessary to reduce the risks associated with users.

Safety of Cloud Services

- Failures

- Dec 14, 2020 A failure of a cloud service caused the linked IoT malfunction, rendering smart keys inoperative and hindering users from entering their houses
- Feb 20, 2021 A failure of a cloud service that lasted for 5 hours, affecting multiple websites
- Feb 26, 2021 A failure of a cloud service affected traffic-related and disaster-prevention-related services
- Mar 11, 2021 A cloud service went down worldwide for approximately one hour and a half
- Apr 1, 2021 A network failure in a cloud service caused multiple websites and services go down
- May 10, 2021 A failure caused by urgent repairs conducted in a cloud service lasted for approximately 5 hours
- Jun 8, 2021 A failure in a CDN service caused the government agencies' websites and other websites go down temporarily
- Jun 23, 2021 A failure related to cloud linkage rendered smartphones inoperative
- Jul 26, 2021 CDN software updating caused a failure
- Sep 2, 2021 A hardware fault in cloud's domestic facilities caused a failure, requiring a few hours to recover from
- Oct 5, 2021 A configuration error in a cloud service caused a 6-hour long failure
- Oct 6, 2021 A network failure of a cloud caused multiple payment services unavailable

Vulnerabilities in IoT devices

- Malfunctioning, hacking or crashing of IoT devices
 - Malfunctioning home eclectic appliances cause a fire, etc.
 - Information concerning privacy being handled
 - Impacts on social infrastructure such as electricity, gas and water
 - Being handled just like conventional home electric appliances
 - Software updating is not as sophisticated as that of PCs and smartphones
 - To be abused as a stepping stone to attacks

Vulnerabilities in IoT devices

- Dec 23, 2020 Several vulnerabilities were found in a manufacturer's "TCP/IP stack", allowing remote code execution attacks
- May 7, 2021 "BadAlloc", a vulnerability to remote code execution attacks was found in RTOS used for IoT devices and control devices
- May 7, 2021 Vulnerabilities found in some of Wi-Fi routers of a domestic manufacturer and it was recommended that the product should not be used
- May 14, 2021
- May 25, 2021 "FragAttacks", a vulnerability that affects almost all Wi-Fi devices
- May 31, 2021 A vulnerability in the specifications of Bluetooth Core and Mesh
- Jul 6, 2021 The FBI issued another alert regarding vulnerabilities in VPN products
- Jul 29, 2021 A vulnerability in a router manufactured by a domestic manufacturer. It was recommended that the product should not be used, instead of repairing.
- Aug 5, 2021 A vulnerability in multiple domestic router software
- Aug 5, 2021 A vulnerability in "NicheStack", an embedded TCP/IP stack

Ransom DDoS attacks related to social situations

- What is a DDoS attack?
 - A malicious attempt to disrupt the normal processing by overwhelming a specific target with a flood of traffic to force a target server to waste its processing capacity and circuit capacity
- How to create a flood of traffic
 - Sent by multiple attackers, special attacking tools, PC malware and bots, reflection (reflective) attacks, IoT bots
 - There have been a number of DDoS attacks that infect vulnerable IoT with malware and send traffic simultaneously from massive number of devices around since the 2016 Summer Olympics Games in Rio de Janeiro, in particular.

Ransom DDoS attacks related to social situations

- Ransom DDoS attack campaigns
 - Ransom DDoS attack campaigns that occurred around the world in October 2019 and then in August 2020 were active again in January, October and November 2021.
 - Like the previous attacks, the multiple attacks were generated mainly by UDP amplification and tended to last 6 to 9 hours, longer than the previous attacks.
 - They targeted various business including financial institutions and telecom companies.
 - There were some cases where the victims of the previous campaigns were targeted again.
- Examples of attacks inside and outside Japan
 - Jan 28 A DDoS attack on a domestic cloud caused a failure (for approximately 3 hours)
 - Feb 1 A DDoS attack on a domestic online service caused a failure (for approximately 7 hours)
 - Sep 4 A DDoS attack on a financial institution in New Zealand

Ransom DDoS attacks related to social situations

- OpMyanmar Campaign by Anonymous
 - Anonymous launched a campaign called OpMyanmar to make a protest against the military coup that occurred in Myanmar in February. Attacks included DDoS attacks on the related websites and website defacements.
 - As Japanese companies are investing in the redevelopment project of the former site of Yangon Military Museum, over 30 websites, including the websites of the LDP, the Japan Federation of Economic Organizations, and the prime minister's official residence were designated as targets.
 - On April 7, Anonymous tweeted that it attacked two of the Japanese websites included in the above list.
- Attacks related to the Tokyo Olympics
 - There have been no cyberattacks that disrupted the games.
(Source: Document 4 from the 31st Meeting of the Cybersecurity Strategic Headquarters (on September 27, 2021))

Ransomware

- Ransomware
 - It encrypts files recorded on HDD by using malware and makes it inaccessible to its users (taken as a hostage). It is distributed widely to increase the impact.
- Standard ransomware
 - It attacks a specific target who is likely to pay a ransom by using ransomware. A ransom tends to be expensive.
- Disclosure ransomware and information leaks
 - Steal information before infecting with ransomware and encrypting it (forwarded externally).
 - Then, take the encrypted information as a hostage and demand a ransom.
 - Furthermore, threaten to disclose the confidential information to a leak website and demand a ransom.
 - There is a leak website for each type of ransomware or a group of hackers has its own.
 - Leak websites are normally on a dark website where the information is disclosed to all those who can access to the dark website since it is designed to disclose information.

Ransomware

- Cases

- An U.S. major petroleum pipeline was infected by ransomware and suspended the operation to confirm the impact
- A major meat processing company was infected by ransomware and suspended the operation, which was restored 3 days later.
- A domestic consultant company for domestic local governments was infected by ransomware, resulting in leaks of information and affecting the entrusted businesses concerning the several local and central government offices.
- A domestic construction consultant suffered a cyberattack and may have had the data on public works stolen.
- A public hospital in Tokushima Prefecture was infected by ransomware.

Overview of IJ Security Business

wizSafe ～Make safety a matter of course～

Realize a future where people can use ICT with peace of mind and without worrying about threats by providing the services with built-in security



wizSafe

安全をあたりまえに

Safety for granted

Support a society

Support the foundation of the whole society, from corporate activities to people's prosperous life by making safety as standard quality and providing stable IT environments.

Increase safety

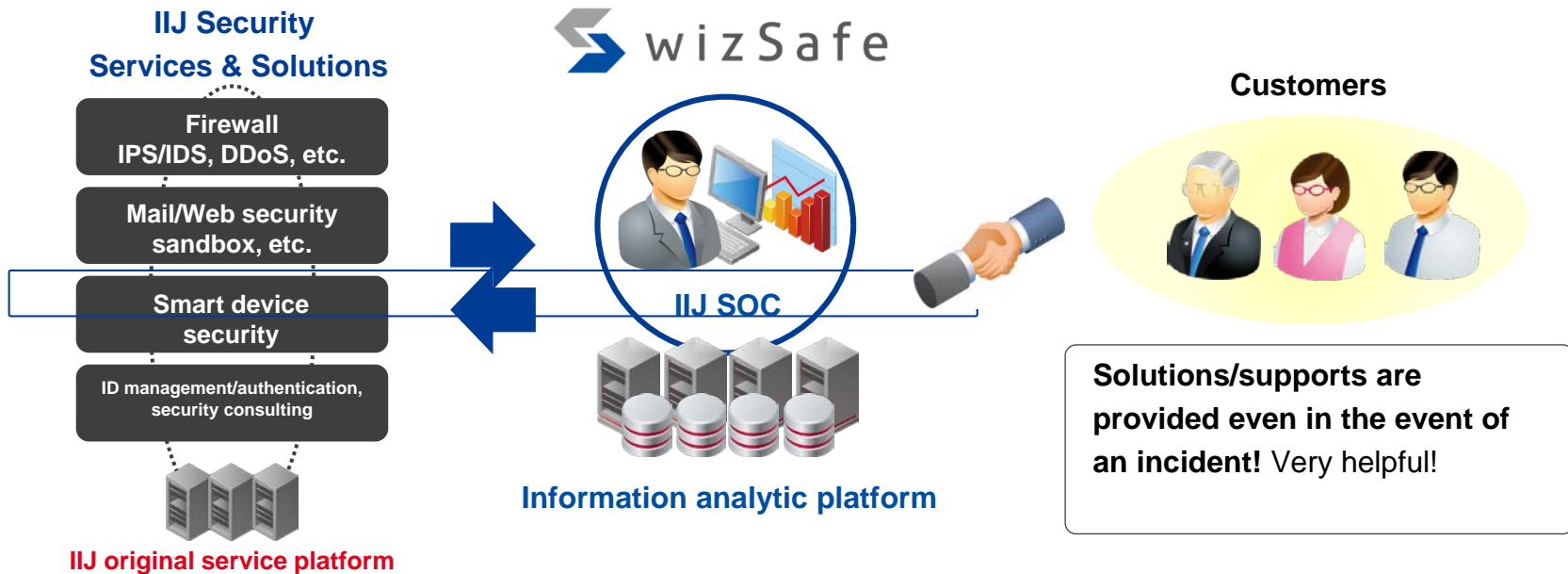
Increase the security level of the whole society by proactively providing the unique information based on the ample database on threats and advanced analytical technology.

Bring reform

Have the foresight to go ahead of the time and bring reform to the base of "IT security" as required without being afraid of changes

Outline of the security business

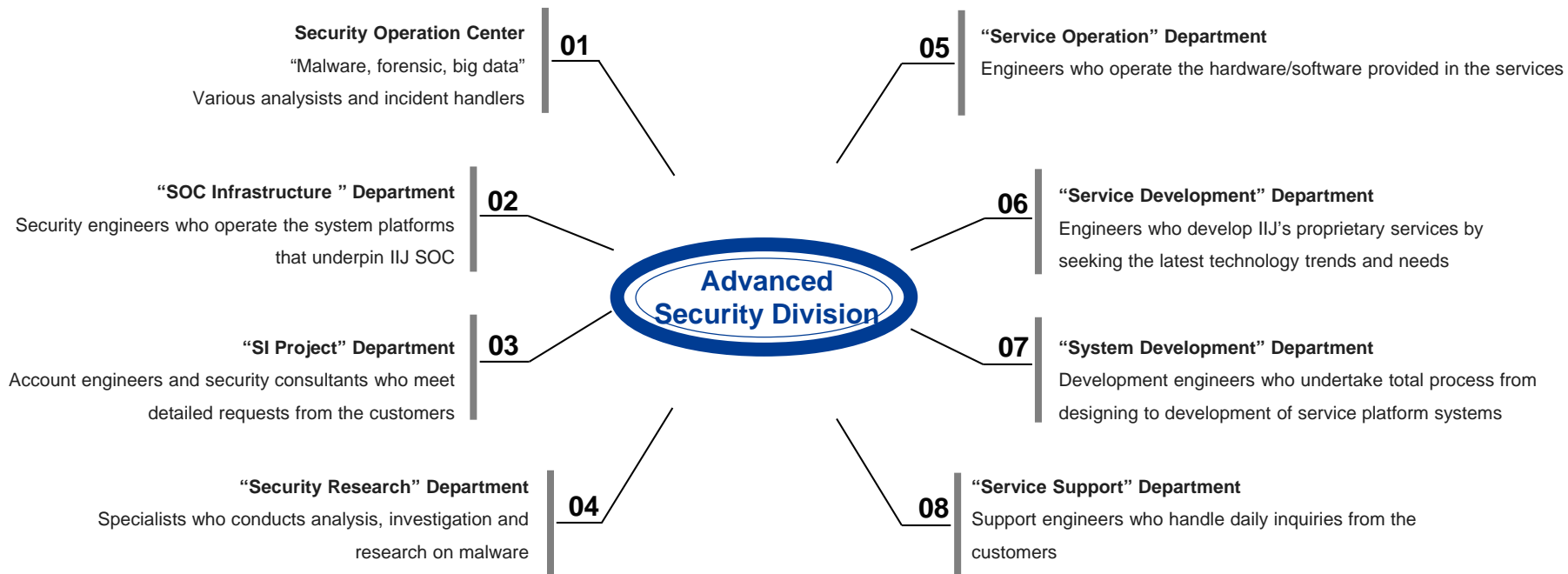
Implement comprehensive support including supports in the event of an incident by providing various services and solutions centering around IIJ SOC



Departments under Advanced Security Division

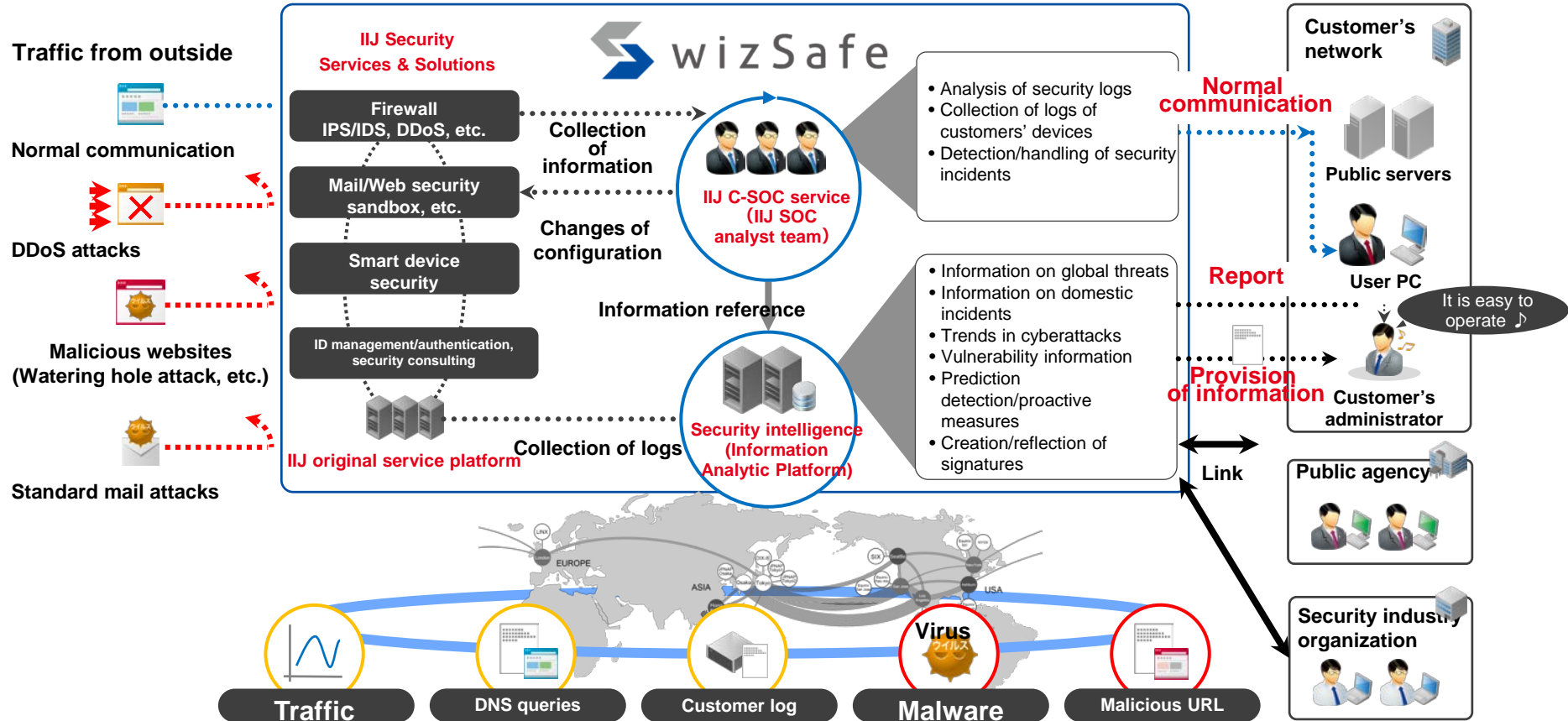
Functions and roles required as an organization for security business are integrated into the division

Parties concerned flexibly cooperate with each other to handle each project depending on the situation.



General view of IJ security business

Integrated operation by IJ SOC



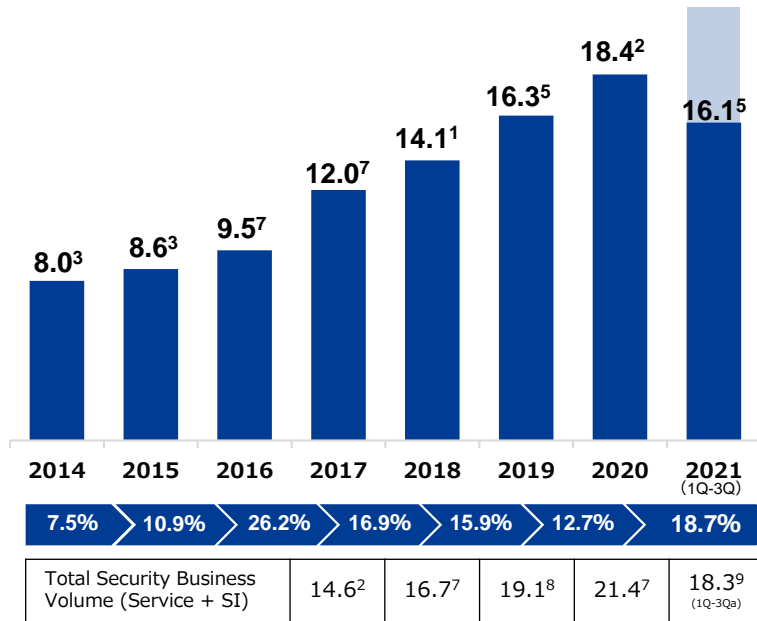
FY2021 Business Overview

Overview of security business

The business has kept growing in double-figures since 2016 when the business reinforcement was launched.

(JPY billion)

Security Service Revenue



Stable stock sales through monthly subscription service

Maintain stable revenues from security services supported by long-standing services including IIJ secure Web gateway service, IIJ secure MX service and IIJ managed firewall service

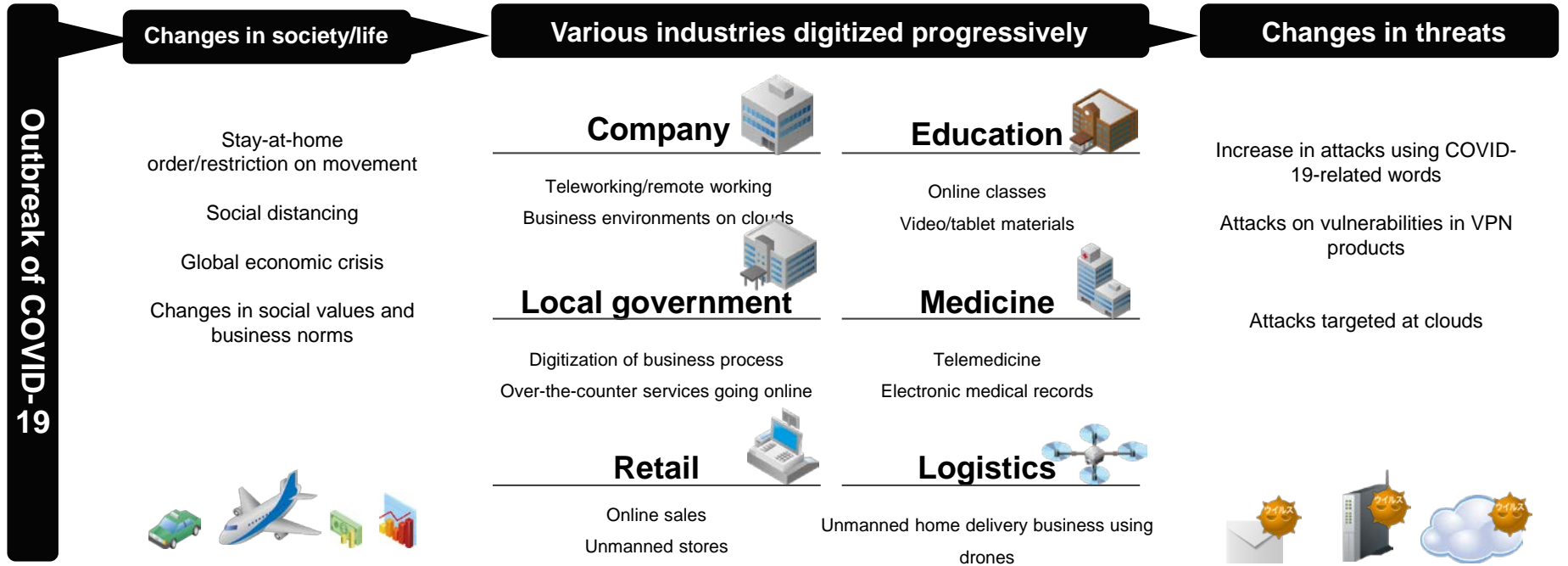
New services meeting new security needs associated with changes in working styles

There has been an increase of teleworking, shift to use of clouds and other changes in working styles and use of ICT due to the COVID-19 pandemic. The growth is maintained by introducing new services catered to these changes.

FY2021 New Services

Changes in the external environments due to the pandemic

Various industries have been digitized progressively and threats have changed accordingly because the society and life have changed due to the COVID-19 pandemic.



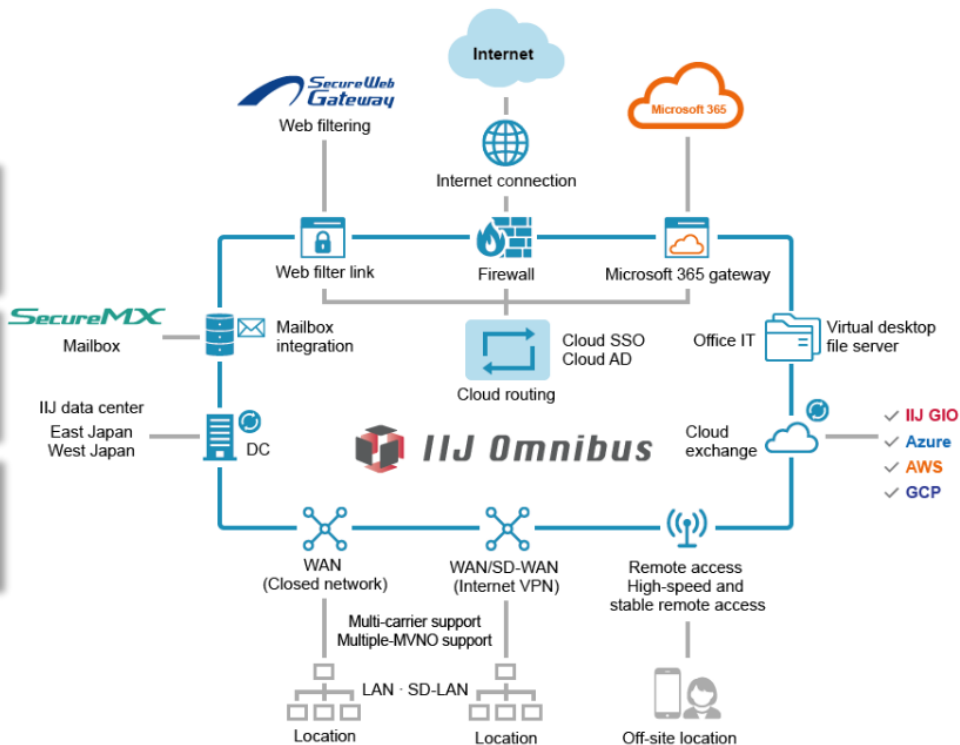
IIJ Flex Mobility Service/ZTNA

One of the services constituting IIJ Omnibus and a remote access service with added function of zero trust network

Enterprise VPN
Optimized comfortable communication

ZTNA
Secured connection control

DEM/ visualization
Grasp detailed usage conditions/risks



IIJ Omnibus is a network cloud brand that covers an entire corporate network

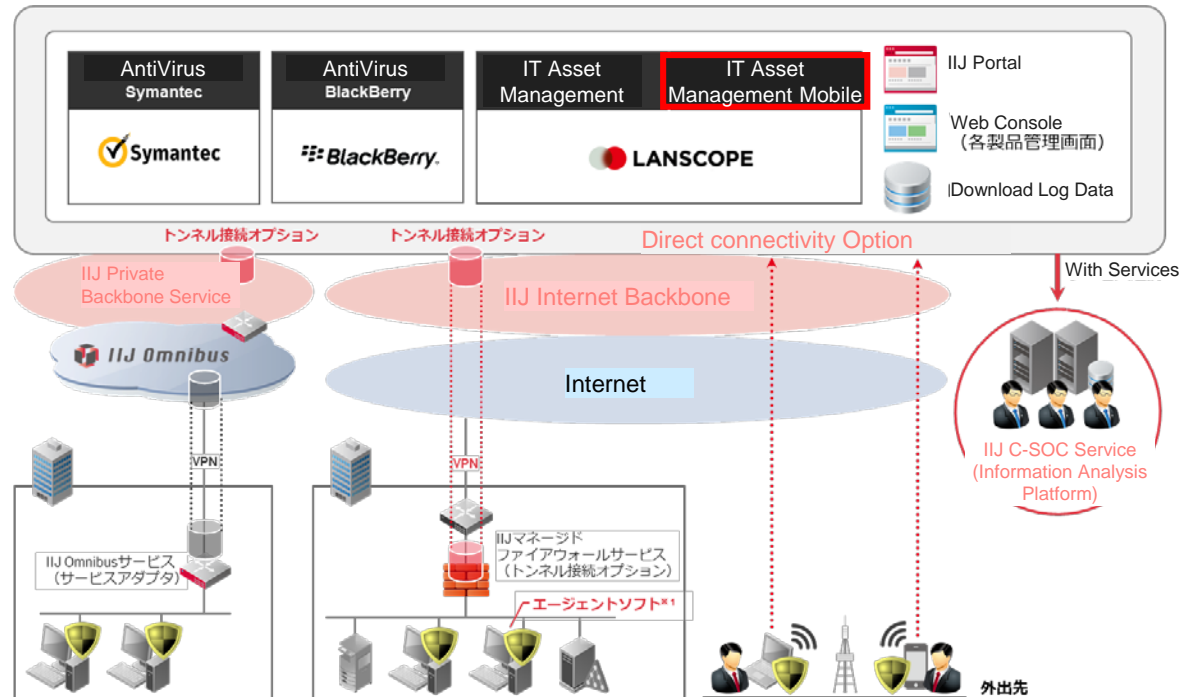
※ZTNA : Zero Trust Network Access
※DEM : Digital Experience Monitoring

IIJ Secure Endpoint Service “IT Asset Management Mobile”

“IT asset management function” and “MDM function” are provided in an integrated manner

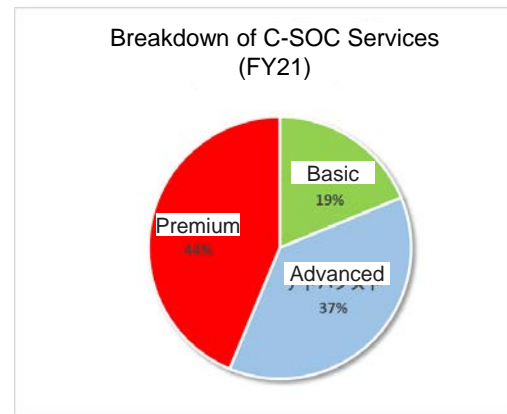
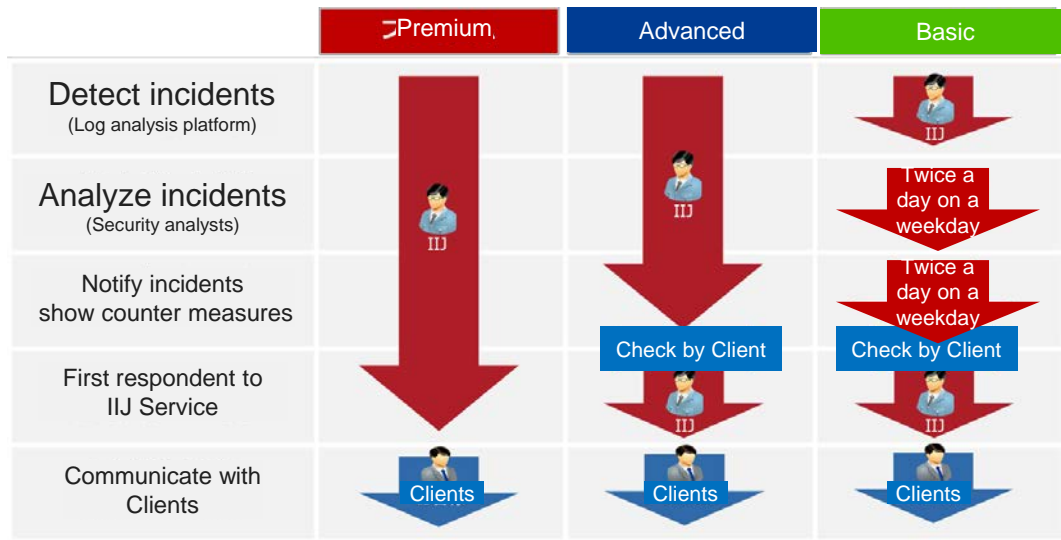
Equipped with comprehensive functions that enable centralized management for PC, iOS and Android

- Improve efficiency of IT asset management using PC, smartphones and tablets through automatic acquisition of asset information and application distribution
- Grasp devices that breach the usage rules of vulnerability
- Able to automatically acquire operation logs of PC, iOS and Android and grasp the usage conditions



IIJ C-SOC Service Premium

Active responses, e.g. blocking unauthorized access
Reduce the burden of security operations and risks of customers through threat hunting for related events by condensing the time to initial action.

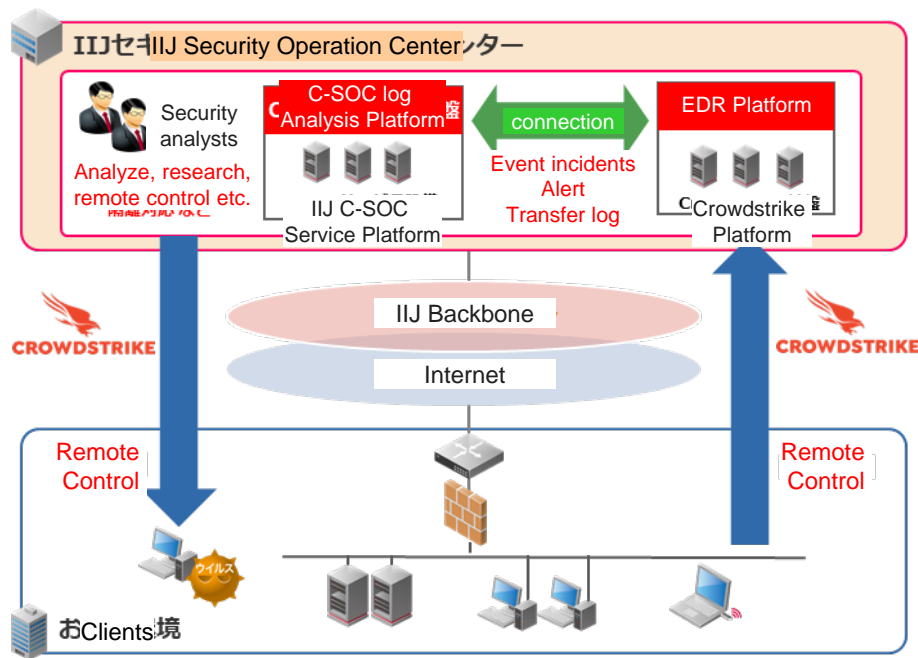


Meet clients' demands with 3 service lineups

IIJ C-SOC Service Premium EDR Operation Options

The service makes an initial response to an incident on behalf of the customer by using the EDR tool (CrowdStrike Falcon) introduced in the customer's device

- Detection not only in the network but also in the client
- Refinement and containment of incidents
- The time to respond to an incident in the client is not required. The customer can focus on after-the-fact responses, such as consideration of measures to prevent reoccurrence



Total support from implementation through operations of the platform for grasping, managing and controlling uses of the cloud services

■ Visualization of shadow IT

- Visualize “who” accesses “which service and when” to grasp the usage conditions of shadow IT that entails possible risks of information leaks and other threats

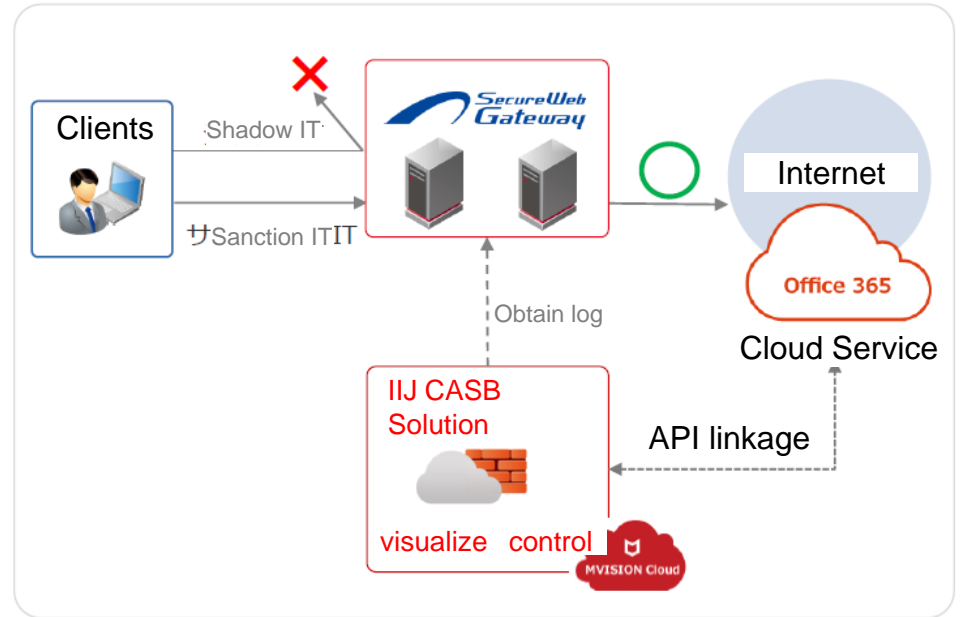
■ Visualization/control of sanction IT

- Visualize the usage conditions by linking the customer's cloud service with API, which will allow isolation of files located on the cloud and deletion of share permissions as required

■ Operation support following the introduction

- In the operation support following the introduction, servers required for log linkages are fully managed. Support for DLP creation is also available.

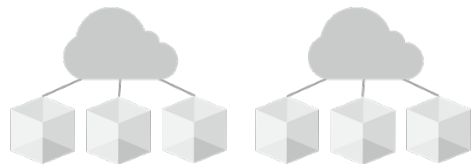
CASB (Cloud Access Security Broker): Visualize and control use of clouds by setting up a single control point among multiple cloud providers



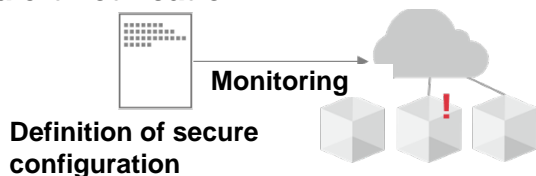
IJ CSPM Solution

It visualize vulnerabilities due to defective IaaS configurations. It reduces security risks specific to clouds through integrated management of different cloud providers.

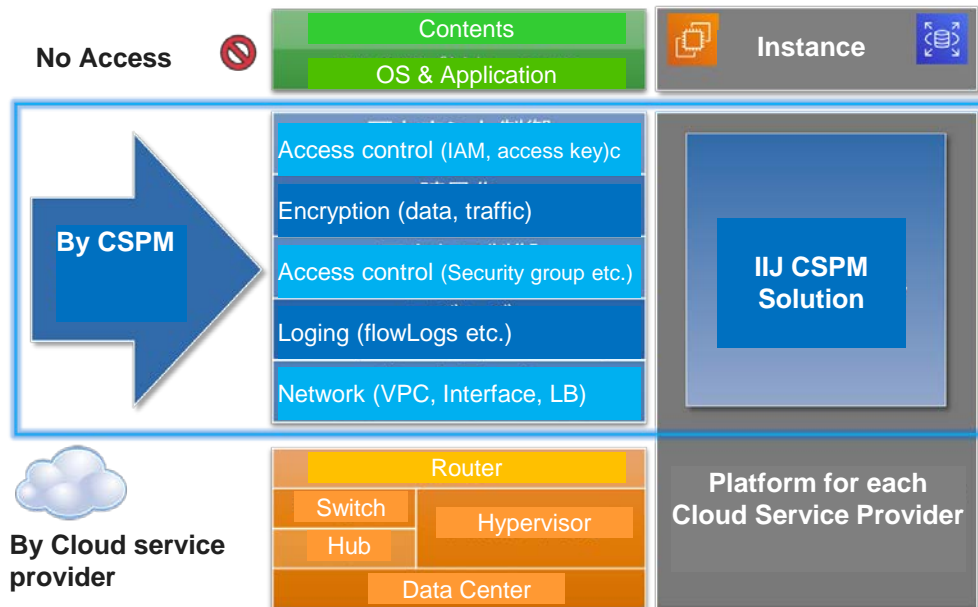
Centralized monitoring of multi-clouds and multi-accounts



Detection of resources that breach the policies and alert notification



Microsoft Azure, AWS and GCP are supported







CSPM (Cloud Security Posture Management): “Cloud security dynamic management” or “status management of concerning cloud configuration”

IJ Security Training School

It provides practical programs based on knowledge gained through security service operations and incident handling at IJ

- Provide knowledge and know-how gained through security operations over years
- Able to learn how to handle the latest security threats and countermeasures
- Learn required knowledge and skills in a short time through practical trainings

	Information Coordinator 	Security Analyst 	Incident Handler 	System Administrator 
Tasks	<ul style="list-style-type: none"> • In charge of communication • In charge of spreading information • Legal advisor 	<ul style="list-style-type: none"> • Researcher • Security strategy • Vulnerability consultant • Self assessment 	<ul style="list-style-type: none"> • Commander • Manage and handle incidents • Forensics • Analyze malware 	<ul style="list-style-type: none"> • IT strategy, system planning • Construction, operation and maintenance of systems & infrastructure • Help desk
High Level			Analyze Malware	Forensics
Advanced	Security Management		Packet and log analysis	Course on incident handling
	Security Risk Compliance		Vulnerability check and management	Course on understanding attack, prevention etc. (Plan to launch in Mar. 2022)
Basic				Secure System Design
	Security platform			

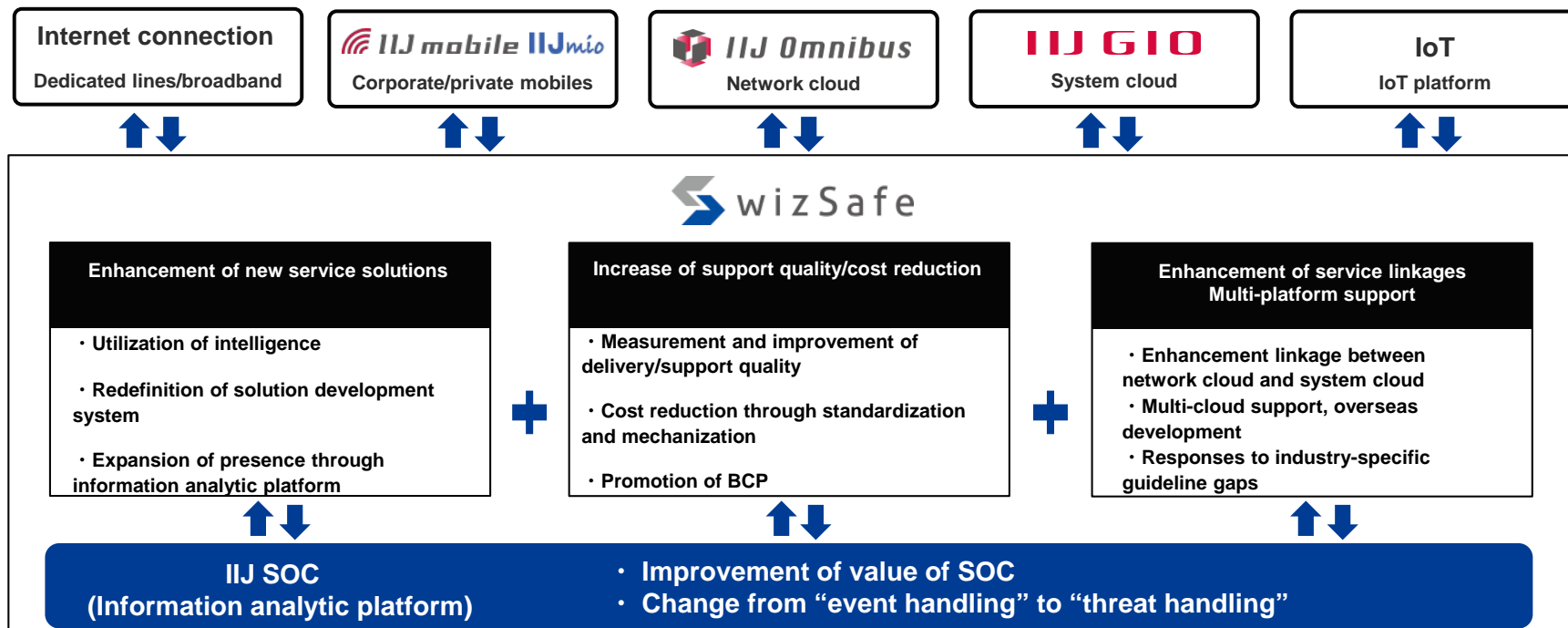


Future outlook for Security Business



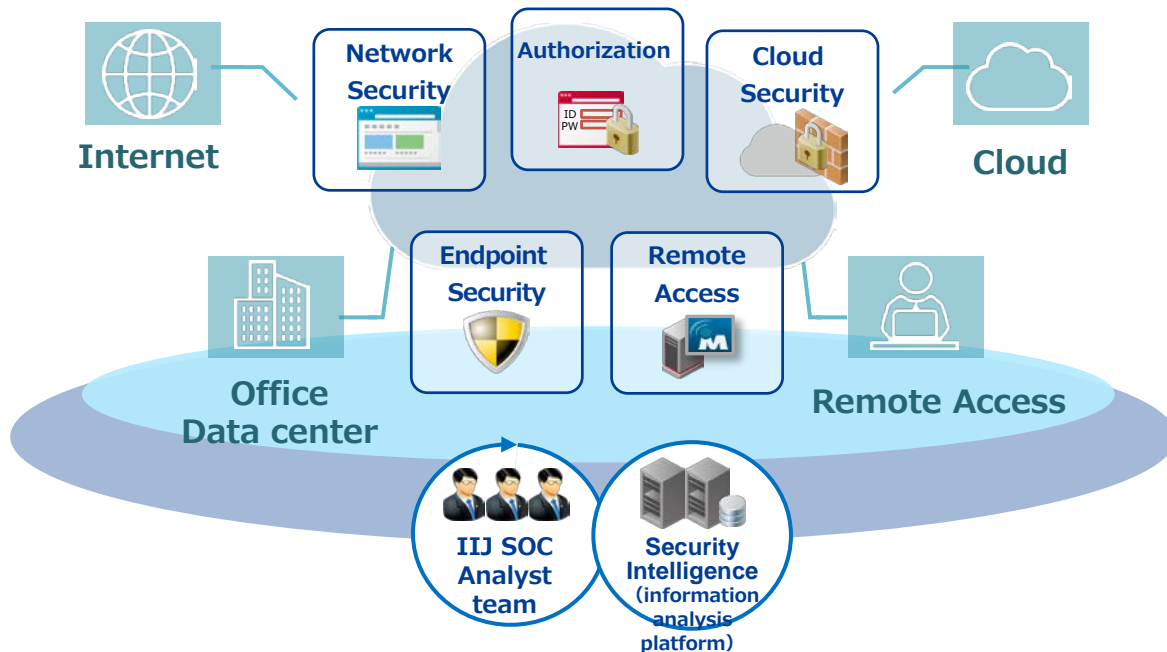
Business Directivities

Enhance linkages with each business domain and expand the required functions and elements aiming at a “state where security elements are incorporated in all kinds of service”



Security supporting Digital Work Place

Without lowering productivity, anyone safely works from wherever with any device. IIJ provides security for work place



New Network Security Services

Network Security to realize Zero Trust environment
which enables to handle information safely anytime and anywhere
Expect to realize ZTN by combining SASE and SOC

